REMARKS/ARGUMENTS

Status of Claims

Claims 1-18 stand rejected.

Claims 1, 3, 5, 9, 11, and 13 are currently amended.

Claims 2, 6, 10, 14, 17, and 18 are hereby canceled.

Claims 19 and 20 are new.

Thus, claims 1, 3-5, 7-9, 11-13, 15, 16, 19, and 20 are pending in this patent application.

The Applicants hereby request further examination and reconsideration of the presently claimed application.

Priority Documents

The Applicants respectfully request that the Examiner indicate on the Office Action Summary whether the certified copies of the priority documents have been received from the International Bureau.

Claim Rejections – 35 U.S.C. § 102

Claims 1-18 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Application Publication 2002/0120760 (*Kimchi*). Claims 2, 6, 10, 14, 17, and 18 have been canceled, claims 3-5, 7, and 8 depend from independent claim 1, and claims 11-13, 15, and 16 depend from independent claim 9. Thus, claims 1, 3-5, 7-9, 11-13, 15, and 16 stand or fall on the application of *Kimchi* to independent claims 1 and 9. According to MPEP § 2131, " [a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." The Applicants respectfully assert that *Kimchi* fails to teach each and every element of independent claims 1 and 9, and consequently fails to anticipate claims 1, 3-5, 7-9, 11-13, 15, and 16.

Kimchi fails to anticipate claims 1, 3-5, 7-9, 11-13, 15, and 16 because *Kimchi* fails to teach that: (1) the authentication center authenticates the terminal, generates a session key for the terminal and the soft switch/signaling proxy, and sends the session key to the soft switch, so as to be distributed to the terminal upon a successful authentication, (2) the authentication center generates a first verification word for the terminal according to a key Kc shared with the terminal, encrypts the session key with the shared key Kc, and returns the encrypted session key and the first verification word to the soft switch, (3) the soft switch returns a registration failure response message to the terminal to notify the terminal of a registration failure, and (4) the terminal generates a second verification word according to the key Kc shared with the authentication center, and sends a registration message containing the second verification word to the soft switch for a registration again. Claims 1 and 9 read:

1. A key distribution method applied in the Next Generation Network comprising a terminal, a soft switch and an authentication center, comprising:

the terminal sending a registration request message to the soft switch for a registration;

the soft switch sending an authentication request message to the authentication center for the authentication for the terminal; and

the authentication center authenticating the terminal, generating a session key for the terminal and the soft switch, and sending the session key to the soft switch, so as to be distributed to the terminal upon a successful authentication;

wherein the step of the authentication center authenticating the terminal comprises:

the authentication center generating a first verification word for the terminal according to a key Kc shared with the terminal, encrypting the session key with the shared key Kc, and returning the encrypted session key and the first verification word to the soft switch;

the soft switch returning a registration failure response message to the terminal to notify the terminal of a registration failure;

the terminal generating a second verification word according to the key Kc shared with the authentication center, and sending a registration message containing the second verification word to the soft switch for a registration again; and

the soft switch authenticating the terminal according to the first verification word and the second verification word.

9. A key distribution method applied in the Next Generation Network comprising a terminal, a signaling proxy, a soft switch and an authentication center, comprising:

the terminal sending a registration request message through the signaling proxy to the soft switch for a registration;

the soft switch sending an authentication request message to the authentication center for the authentication for the terminal; and

the authentication center authenticating the terminal, generating a session key for the terminal and the signaling proxy, and sending the session key to the soft switch, so as to be distributed through the signaling proxy to the terminal upon a successful authentication;

wherein the step of the authentication center authenticating the terminal comprises:

the authentication center generating a first verification word for the terminal according to a key Kc shared with the terminal and a key Ksp shared with the signaling proxy, encrypting the session key respectively with the shared key Kc and the shared key Ksp, and returning the encrypted session key and the first verification word to the soft switch;

the soft switch returning a registration failure response message through the signaling proxy to the terminal to notify the terminal of a registration failure;

the terminal generating a second verification word according to the key Kc shared with the authentication center, and sending a registration message containing the second verification word to the signaling proxy to be forwarded to the soft switch for a registration again; and

the soft switch authenticating the terminal according to the first verification word and the second verification word.

(Emphasis added). First, claims 1 and 9 recite that the authentication center authenticates the terminal, generates a session key for the terminal and the soft switch/signaling proxy, and sends the session key to the soft switch, so as to be distributed to the terminal upon a successful authentication. In contrast, *Kimchi* sends his session key **directly to his client (e.g. the terminal)**:

1. Client generates x, a random string, and does MD5 hash on x concatenated with its password p, the location I (same parameter provided in Online.location).

2. The client then sends the result of (1) in the Online.key transaction parameter.

3. **The server** passes the hash and x into the database, to validate the password. Then **generates a session key sk**, and XORs it with the password hash (without x), **and send it in the Online.accept PDU**, along with the (normal) session ID. The server then appends the PDU with authentication token, created by concatenating the PDU string (starting with the /tgp, and ending with the ")", before applying

HTTP encoding, if any) with the session key, and hashes using MD5. **The client opens the session key** (by XORing it back with h(p)), and validates the authentication token.

Kimchi, ¶¶ 277-279 (emphasis added). As shown above, *Kimchi* sends his session key directly to his client (e.g. the terminal), rather than sending the session key to the soft switch so as to be distributed to the terminal upon a successful authentication. Thus, *Kimchi* fails to teach that the authentication center authenticates the terminal, generates a session key for the terminal and the soft switch/signaling proxy, and sends the session key to the soft switch, so as to be distributed to the terminal upon a successful authentication.

Second, claims 1 and 9 recite that the authentication center generates a first verification word for the terminal according to a key Kc shared with the terminal, encrypts the session key with the shared key Kc, and returns the encrypted session key and the first verification word to the soft switch. Such a limitation requires **two keys**: a key Kc shared with the terminal and the session key generated by the authentication center. In contrast, *Kimchi* only has **one key (the session key)** in his client-server exchange:

> 1. Client generates x, a random string, and does MD5 hash on x concatenated with its password p, the location I (same parameter provided in Online.location).
>
> 2. The client then sends the result of (1) in the Online.key transaction parameter.
>
> 3. The server passes the hash and x into the database, to validate the password. Then generates **a session key sk**, and XORs it with the password hash (without x), and send it in the Online.accept PDU, along with the (normal) session ID. The server then appends the PDU with authentication token, created by concatenating the PDU string (starting with the /tgp, and ending with the ")", before applying HTTP encoding, if any) with **the session key**, and hashes using MD5. The client opens **the session key** (by XORing it back with h(p)), and validates the authentication token.

Kimchi, ¶¶ 277-279 (emphasis added). As shown above, *Kimchi* only has one key (the session key) in his client-server exchange, whereas the pending claims require two keys. Thus, *Kimchi*

fails to teach that the authentication center generates a first verification word for the terminal according to a key Kc shared with the terminal, encrypts the session key with the shared key Kc, and returns the encrypted session key and the first verification word to the soft switch.

Third, claims 1 and 9 recite that the soft switch returns a registration failure response message to the terminal to notify the terminal of a registration failure. As discussed above, *Kimchi* does not use a soft switch in his client-server exchange. *See, e.g., Kimchi,* ¶¶ 277-279. Thus, *Kimchi* cannot teach that the soft switch returns a registration failure response message to the terminal to notify the terminal of a registration failure.

Fourth, claims 1 and 9 recite that the terminal generates a second verification word according to the key Kc shared with the authentication center, and sends a registration message containing the second verification word to the soft switch for a registration again. As discussed above, *Kimchi* does not use a soft switch in his client-server exchange. *See, e.g., Kimchi,* ¶¶ 277-279. Thus, *Kimchi* cannot teach that the terminal generating a second verification word according to the key Kc shared with the terminal generates a second verification word according to the key Kc shared with the authentication center, and sends a registration message containing the second verification word to the soft switch for a registration again. As such, *Kimchi* fails to teach at least one element of independent claims 1 and 9, and consequently fails to anticipate claims 1, 3-5, 7-9, 11-13, 15, and 16.

New Claims

New claims 19-20 recite novel and non-obvious aspects of the invention. Specifically, the cited prior art fails to teach a key distribution system applied in the Next Generation Network comprising: a terminal adapted to send a registration request message for a registration; a soft switch adapted to receive the registration request message sent from the terminal and sent an

authentication request message for the authentication for the terminal; and an authentication center adapted to receive the authentication request message sent from the soft switch, to authenticate the terminal, to generate a session key for the terminal and the soft switch, and to send the session key to the soft switch so as to be distributed to the terminal upon a successful authentication; wherein the authentication center is further to adapted to generate a first verification word for the terminal according to a key Kc shared with the terminal, to encrypt the session key with the shared key Kc, and to return the encrypted session key and the first verification word to the soft switch; wherein the soft switch is further to adapted to return a registration failure response message to the terminal to notify the terminal of a registration failure, and to authenticate the terminal according to the first verification word and a second verification word; and wherein the terminal is further to adapted to generate the second verification word according to the key Kc shared with the authentication center, and to send a registration message containing the second verification word to the soft switch for a registration again. In addition, the cited prior art fails to teach a key distribution system applied in the Next Generation Network comprising: a terminal adapted to send a registration request message for a registration; a signaling proxy adapted to forward the registration request message from the terminal, and to distribute a session key to the terminal; a soft switch adapted to receive the registration request message sent from the terminal through the signaling proxy and sent an authentication request message for the authentication for the terminal; and an authentication center adapted to receive the authentication request message sent from the soft switch, to authenticate the terminal, to generate the session key for the terminal and the signaling proxy, and to send the session key to the soft switch so as to be distributed through the signaling proxy to the terminal upon a successful authentication; wherein the authentication center is further adapted to generate a first verification word for the terminal according to a key Kc shared with the

terminal and a key Ksp shared with the signaling proxy, to encrypt the session key respectively with the shared key Kc and the shared key Ksp, and to return the encrypted session key and the first verification word to the soft switch; wherein the soft switch is further adapted to return a registration failure response message through the signaling proxy to the terminal to notify the terminal of a registration failure, and to authenticate the terminal according to the first verification word and a second verification word; and wherein the terminal is further adapted to generate the second verification word according to the key Kc shared with the authentication center, and to send a registration message containing the second verification word to the signaling proxy to be forwarded to the soft switch for a registration again. Thus, new claims 19 and 20 are allowable over the cited prior art.

Finality of Next Office Action

The Applicants would like to point out that claim 2 and 10 have been rewritten in independent form by incorporating the limitations of claims 2 and 10 into claims 1 and 9, respectively. The Applicants would also like to remind the Examiner of the rules regarding finality of office actions. Specifically, MPEP § 706.07(a) states that the next office action should not be final if the Examiner changes the grounds of rejection for any of claims 1, 3, 4, 7-9, 11, 12, 15, and 16. Should the Examiner insist on making the next office action final and including a new ground of rejection for any of claims 1, 3, 4, 7-9, 11, 12, 15, or 16, the Applicants request a telephone conference with the Examiner and the Supervisory Patent Examiner to clarify the finality issue, and thereby potentially avoid a petition under 37 C.F.R. § 1.181.
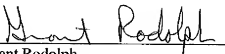
CONCLUSION

Consideration of the foregoing amendments and remarks, reconsideration of the application, and withdrawal of the rejections and objections is respectfully requested by the Applicants. No new matter is introduced by way of the amendment. It is believed that each ground of rejection raised in the Office Action dated December 24, 2009 has been fully addressed. If any fee is due as a result of the filing of this paper, please appropriately charge such fee to Deposit Account Number 50-1515 of Conley Rose, P.C., Texas. If a petition for extension of time is necessary in order for this paper to be deemed timely filed, please consider this a petition therefore.

If a telephone conference would facilitate the resolution of any issue or expedite the prosecution of the application, the Examiner is invited to telephone the undersigned at the telephone number given below.

Respectfully submitted,
CONLEY ROSE, P.C.

Date: 2/24/10

Grant Rodolph
Reg. No. 50,487

5601 Granite Parkway, Suite 750
Plano, TX 75024
(972) 731-2288
(972) 731-2289 (Facsimile)

ATTORNEY FOR APPLICANTS